



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,010	12/15/1999	PIERRE CALVEZ	6313	3226

7590 06/03/2004

EDWARD J KONDRACKI  
MILES & STOCKBRIDGE PC  
1751 PINNACLE DRIVE  
SUITE 500  
MCLEAN, VA 221023833

EXAMINER

AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/03/2004

14

Please find below and/or attached an Office communication concerning this application or proceeding.

14

# Office Action Summary

Application No.

09/461,010

Applicant(s)

CALVEZ ET AL.

Examiner

Tracey Akpati

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 20-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 20-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 December 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1-29 and 31-52 have been amended. Claims 53 and 54 have been added. The attorney's argument necessitated new grounds of rejection. This action is a non-final.

#### *Response to Arguments*

2. *With respect to Claim 47, the attorney argues that Ishii fails to teach "the construction of a local registration authority and the construction of automating the process."* The tamper resistant, personal portable device represents the local registration authority. This is because the personal portable device is in communication with the key generating center(s) and requests the creation of a key pair, after the user enters his/her personal information (see Fig. 4 and column 7, lines 64-67, column 8, lines 1-3).

The process of creating and/or certificate of at least one pair of keys is automated. Figure 4 clearly shows that after the user enters his/her personal information, the key pair and certificate is generated without any user intervention. Hence, the process is automated.

---

3. *With respect to Claim 52, the attorney argues that Ishii does not disclose symmetric keys.* Claim 52 has been amended from a 102 to a 103 to show obviousness of having a symmetric key system within Ishii's invention. The attorney should however note that a secret key cyptosystem is the same thing as a symmetrical cryptosystem. A secret/symmetric key cryptosystem uses the same key (secret key) to encrypt and decrypt its information. Ishii discloses a symmetrical key system on column 1, lines 26-29 and furthermore its advantage over an asymmetrical cryptosystem on column 1, lines 30-37, which is a higher processing speed. Hence for a faster

Art Unit: 2135

computing/processing speed, the symmetrical system can be substituted for the asymmetrical system disclosed also in Ishii on column 11, lines 50-67 and column 12, lines 1-46. A symmetrical cryptosystem is also well known in the art.

4. *With respect to Claim 20, the attorney argues that Van Oorschot on column 3, line 24-33 does not teach the limitation of "searching in storage means for at least one subject for which a pair of asymmetric keys and an associated certificate must be created."* The examiner agrees with the attorney and hence a new reference has been introduced. Smith et al discloses this limitation on column 5, lines 29-35. In Smith, the client information is stored and retrieved (when being compared), afterwards the key pair is generated.

5. With respect to Claim 29, its limitation is now met by Smith et al on column 5, lines 38-52.

---

6. *With respect to Claim 51 and 52, the attorney argues that the art used to reject limitation is directed at an asymmetrical system.* The examiner's rebuttal can be found above, in Claim 47 rebuttal.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 47, 48, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389).

With respect to Claim 47 the limitation “a computer system for creating and managing pairs of asymmetrical cryptographic keys and certificates associated with the pairs of keys, the pairs of keys and the certificates being intended for subjects managed by said system, comprising a key generating center for creating at least one pair of keys at the request of a local registration authority with which the key generating center communicates; at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority and means for automating the creation and/or certification of at least one pair of keys for each subject managed by the system” is met by Ishii on column 5, lines 44-67, column 8, lines 8-24 and Fig. 2. In the cited reference, there exists a secret key(private key) generation unit, a public key generation unit and a certification production

---

unit. The tamper resistant personal device represents the local registration authority. It is in communication with the key-generating center. The key-generating center is both the secret/private and public generating center (see Fig. 2). After the user's personal information is entered, the personal device communicates with the other modules within to generate the key pairs and certificate.

Hence, it would have been obvious to have the tamper resistant personal device as the local registration authority because the personal portable device is in communication with the key generating center(s) and requests the creation of a key pair, after the user enters his/her personal information (see Ishii, Fig. 4 and column 7, lines 64-67, column 8, lines 1-3). Furthermore it is obvious that the process of creating and/or certificate of at least one pair of

Art Unit: 2135

keys is automated because Figure 4 clearly shows that after the user enters his/her personal information, the key pair and certificate is generated without any user intervention. Hence, the process is automated.

With respect to Claim 48, the limitation “a central management service for creating, updating and consulting objects and subjects managed by said system a local registration authority for handling the creation and/or the certification of keys intended for the objects and the subjects a central security base containing the subjects and the objects managed by the system with which the local registration authority communicates a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; and at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority” is met by Ishii on Figure 5.

---

With respect to Claim 52, the limitation “a computer system for creating symmetrical cryptographic keys, wherein a symmetrical cryptographic key can be used to both encode and decode data” is met by Ishii on column 1, lines 26-29; and wherein said system manages subjects, characterized in that it comprises a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority and means for automating the

Art Unit: 2135

creation of at least one key for each subject managed by the system” is met by Ishii on column 11, lines 50-67 and column 12, lines 1-46.

Claims 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Van Oorschot (6370249 B1).

With respect to Claims 49 and 50, all the limitation is met by Ishii except the limitation below.

The limitation of “a wake up mechanism periodically waking up the local registration authority” is met implicitly by Van Oorshot on column 3, lines 14-19. The time-to-time provision of a public key to a client implicitly discloses that the system would need to be alert from at these frequent time intervals and hence this necessitates a wake up mechanism.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorshot within the system of Ishii because a wake up mechanism is necessary for continuous generation and replacement of old keys and certificates, hence yielding a more current, more secure key generation system.

Claims 20, 21, 29, 30, 33, 45, 46, 51, 53, 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Smith (6651166 B1).

With regards to Claim 20, the limitation “creating at least one first individual creation and certification request for a pair of asymmetric keys for said subject” is met by Ishii on column 11, lines 31-33 and 63-67.

The limitation “transmitting a key generation request corresponding to said first individual creation :

Art Unit: 2135

certification request to a key generating center (8), which issues a pair of asymmetric keys in accordance with said key generation request” is met by Ishii on column 11, lines 20-62.

The limitation “creating at least one second individual certification request the public key created for said subject” is met by Ishii on column 11, lines 63-67.

The limitation “transmitting a certification authority request corresponding to said second individual certification request to a certification authority, and issuing a first certificate in accordance with said certification authority request” is met by Ishii on column 12 on lines 12-16, 42-46. Further limitation of “creating a public key for said subject” is met by Ishii on column 11, lines 60-62. Ishii however does not disclose searching a storage means for the subject that needs the asymmetric keys. This is however disclosed by Smith et al.

The limitation “searching in storage means (7) for at least one subject for which a pair of asymmetric keys and an associated certificate must be created” is met by Smith et al on column 5, lines 29-35. In Smith, the client information is stored and retrieved (when being compared), afterwards the key pair is generated.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because retrieval of the subject’s data from storage is a necessary step towards creation of a pair of keys and a corresponding certificate.

With respect to Claim 21, the limitation of “creating a pair of keys for a given subject when said subject lacks a pair of keys and a corresponding first individual creation and



Art Unit: 2135

certification request” is met by Ishii in column 4, lines 16-36; column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20.

With respect to Claim 29, the limitation “creating at least one individual certification request for certifying a public key” is met by Ishii on column 11, lines 63-67.

The limitation “transmitting a certification authority request corresponding to said individual certification request to a certification authority, and issuing a certificate in accordance with said certification authority request” is met by Ishii on column 12, lines 12-16 and 42-45. Ishii however does not disclose searching the storage means for a pair of asymmetric keys. This is disclosed by Smith et al.

The limitation “searching in storage means (7) for at least one pair of asymmetric keys for the public key for which a certificate must be created” is met by Smith et al on column 5, lines 38-52.

---

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because referring back to an already secure storage means for the necessary keys allows the system to save the time it would have used to request and authenticate the sender of the keys from a remote area.

With respect to Claim 30, the limitation “certificate for a given subject when said subject lacks a certificate and an individual certification request” is met by Ishii on column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20.

With respect to Claims 33, the limitation “creating the certificate for a given subject when the certificate expires during this period” is met by Ishii on column 12, lines 17-50.

With respect to Claim 45, the limitation “comprising performing the encoding of one or more extensions in accordance with one or more given rules and of entering the encoded extension or extensions into the individual certification request during the creation of said individual certification request” is met by Ishii on column 11, lines 63-67 and column 12, lines 1-3.

With respect to Claim 46, the limitation “changing the value of an attribute contained in each of the individual first and second requests to indicate status of the process” is met by Ishii on Fig. 20 and 21.

---

With respect to Claim 51, the limitation “creating at least one individual request for creating a symmetric key for said subject” is met by Ishii on column 1, lines 26-29, column 11, lines 20-21 and 31-33. A secret key cryptosystem is the same thing as a symmetrical cryptosystem because of the use of the same key to encrypt and decrypt. These symmetrical keys, as disclosed on column 1 are much faster than their asymmetrical counterparts. Hence for the advantage of increasing processing speed, they can intuitively be substituted for the asymmetrical keys in the invention disclosed on column 11.

The limitation “transmitting a key generating request corresponding to said individual creation request to a key generating center (8)” is met by Ishii on column 11, lines 31-33.

The limitation “issuing by said key generating center a symmetric key in accordance with said transmitted key generating request” is met by Ishii on column 11, lines 35-62. Ishii however does not disclose a storage means as disclosed below.

The limitation “searching in storage means (7) for at least one subject for which a symmetric key must be created” is partly met by Smith et al on column 5, lines 29-35. In Smith et al, this input information is retrieved from the SDCE server before the key pair is generated.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii as to achieve high speed processing.

With respect to Claim 53 and 54, the limitation of “creating a pair of keys for a given subject when a certificate issued in response to a certification authority request for a pair of keys for said subject intended for an identical use has been revoked and a new pair of keys been requested” is met by Ishii on column 28: 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20. Revocation will occur intuitively if the device/key(s) is lost/stolen/destroyed, hence the need to reissue/create a new set of keys. The secret key is reproduced first and the public key is reproduced shortly afterwards.

Claims 22, 31, 32, 34, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Smith (6651166 B1) in further view of Van Oorschot (6370249 B1).

With respect to Claim 22, the combination of Ishii and Smith et al meets all the limitation except that of periodical generation of keys and certificates.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii and Smith et al because a periodical generation of new keys provides a more secure computer system as shown by Menezes on page 183, section 8.10. Menezes states that the longer a key is used, the greater chance it will be compromised and the greater the loss.

With respect to Claim 31 and 32, the combination of Ishii and Smith et al meets all the limitation except that of periodically executing the process.

---

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii and Smith et al because a periodical generation of new keys provides a more secure computer system as shown by Menezes on page 183, section 8.10. Menezes states that the longer a key is used, the greater chance it will be compromised and the greater the loss.

With respect to Claims 34, 35 the limitation "creating the new certificate for a given subject when the first certificate expires" is met by Ishii on column 12, lines 17-50.

Claims 23, 24, 25, 26, 27, 28, 36, 37, 38, 39, 40, 41, 42, 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Smith (6651166 B1) in further view of Van Oorschot (6370249 B1).

With respect to Claim 23-25, the combination of Ishii and Smith et al meets all the limitation except that described below.

The limitation “wherein each individual first and second request is created from corresponding multiple creation and certification requests stored in the storage means...” is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii and Smith et al so allow for the secure creation of keys for the required authorized individual.

---

The combination of Ishii, Smith et al and Van Oorschot however does not disclose a set of subjects belonging to a preset list. This is however disclosed by Aziz.

The limitation “...relative to a set of subjects belonging to a preset list or to a set of subjects defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question” is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii, Smith et al and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

Art Unit: 2135

With respect to Claims 26-28, the combination of Ishii, Smith et al and Aziz meets all the limitation except that of searching for the subject that required the new keys.

The limitation "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created" is met by Van Oorschot on column 4, lines 37-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot to the combination of Ishii, Smith et al and Aziz so as to find the correct and authorized recipient of the keys, and hence prevent the sending of keys to an unauthorized individual.

With respect to Claim 36-39, the combination of Ishii and Smith et al meets all the limitation except the limitation disclosed below.

---

The limitation "creating each individual request from a corresponding multiple certification request recorded in the storage means..." is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Van Oorschot to the combination of Ishii and Smith et al so as to allow for the secure creation of keys for the required authorized individual.

The combination of Ishii, Smith and Van Oorschot do not disclose the set of keys belonging to a preset list of keys. This is however disclosed by Aziz.

The limitation "...relative to a set of pairs of keys for subjects belonging to a preset list or to a set of pairs of keys for subjects defined by predetermined criteria, as well as to associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii, Smith et al and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

With respect to Claims 40-43, all the limitation is met by the combination of Ishii, Smith et al and Aziz. The limitation "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created" is met by Van Oorschot on column 4, lines 37-47.

---

It would have been obvious to one of ordinary skill in the art to combine the teachings of Van Oorschot to the combination of Ishii, Smith et al and Aziz so as to allow for the creation and distribution of secure keys.

Claim 44 rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Smith et al (6651166 B1) in further view of Schneier.

With respect to Claim 44, the combination of Ishii and Smith et al meets all the limitation except for the limitation disclosed below.

The limitation "wherein each multiple request comprises an attribute relative to at least one execution date and in that said process consists of including in the search only the multiple requests whose expiration date has arrived" is met by Schneier on page 183-184, section 8.10.

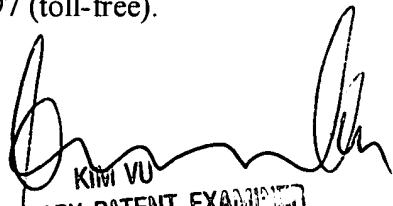
It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schneier within the combination of Ishii and Smith et al so as to prevent the existence of keys for an extended period of time and hence lessen the likelihood of the keys being compromised as disclosed by Schneier within the same citation.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100